Guidance on Cyber Security Arrangements

for 2022/23 Annual Audits

AUDIT SCOTLAND

Prepared by Professional Support for auditors in all sectors

22 February 2023

Contents

Introduction

Purpose of guidance

1. This guidance from Professional Support is intended to assist auditors consider risks related to cyber security at audited bodies as part of 2022/23 core annual audit activity. Cyber security is the practice of defending networks and information systems against malicious attacks designed to compromise access to these systems.

2. This guidance provides information on the current landscape of cyber resilience assessment frameworks within the Scottish public sector, and provides guidance on auditors' consideration of them. This includes:

- the ongoing refresh of the Scottish Government (SG) Public Sector Cyber Resilience Framework (PSCRF)
- the EU Network and Information Systems Regulations 2018 (NIS), and
- the Public Services Network (PSN) and the migration to Future Networks for Government (FN4G) programme.

Background

3. The Guidance on Planning 2022/23 Annual Audits (at paragraphs 82 to 84) highlights that there continues to be a significant risk of cyber-attacks to public bodies, and it is important that they have appropriate cyber security arrangements in place. It advised auditors to consider risks related to cyber security at audited bodies.

4. As reliance on technology grows within audited bodies, failure of network and information systems has a bigger impact on the delivery of public services. In addition, there are more opportunities to compromise those systems. All public bodies need to recognise these cyber threats and embrace the importance of protecting data and securing information.

5. However, as explained in the planning guidance, the revised ISA (UK) 315 includes enhanced requirements for auditors to understand a body's use of IT in its business, the related risks and the system of internal control addressing such risks. Meeting these additional requirements is likely to be sufficient consideration of cyber security in 2022/23. This guidance is intended to assist auditors in that regard.

Consulting with Professional Support

6. Auditors should consult with Professional Support by sending an email to TechicalQueries@Audit-Scotland.gov.uk.

The Frameworks

Public Sector Cyber Resilience Framework – Version 2.0

7. There are many cyber security standards used to assess the level of compliance and accreditation across different aspects of the public sector in Scotland. The PSCRF was created as an aggregation of controls across these standards to provide a more unified approach. In recognition that many of these standards have been improved and refreshed since the original publication, the SG is currently refreshing the controls in the PSCRF to reflect the changes and revisions in the standards that it aggregates. Version 2 of the PSCRF is due to be published before 31 March 2023 with bodies expected to adopt it as the primary cyber security assessment during 2023/24. (For a full list of the standards aggregated by the PSCRF see appendix 2).

8. A significant change in PSCRF Version 2 is the simplification of the control framework; all controls are classified into 1 of 2 tiers. The SG's expectation is that all bodies should adopt all Tier 1 controls; in addition, those that are subject to the EU Network and Information Systems Regulations 2018 (NIS), such as NHS boards and Scottish Water, and those holding sensitive data are also expected to adopt all Tier 2 controls. (Note that adoption of the PSCRF is only on an advisory basis with local government and associated organisations).

9. In addition to simplifying the overall control framework, this refresh has also facilitated the inclusion of additional control areas covering new and emerging technologies, and where experience has identified that the original PSCRF controls could be improved. These new categories introduce controls that allow management to assess risks related to:

- cloud-based services, which have been increasingly adopted and are also key to the support of home-based and hybrid working
- growth in the use of the Internet of Things (IoT), where the variety of web-enabled devices that are in regular use has increased the number of access points via which "bad actors" can gain access to, and potentially compromise, data
- Supply Chain Management, where the need to gain assurance over suppliers of technology solutions was not adequately addressed.

EU NIS Regulations 2018

10. The EU Network and Information Systems Regulations 2018 (NIS Regulations) sets out one comprehensive set of cyber security controls. It provides legal measures to boost the overall level of security of network and information systems for organisations that are defined as “operators of essential services” (OES). In its role as national technical authority for cyber security, the National Cyber Security Centre (NCSC) developed the initial NIS Cyber Assessment Framework (NIS-CAF) in 2018. This was one of the standards aggregated into the PSCRF.

11. A refreshed version of the NIS-CAF (Version 3.1) has been published, with the UK Cyber Security Strategy recommending that this will be used as the common approach to cyber security assessment. Version 2.0 of the PSCRF will encompass all the controls included in Version 3.1 of the NIS-CAF for Tier 2 organisations.

12. Public sector OES in Scotland are defined as NHS boards and Scottish Water. They are subject to the NIS Regulations, requiring an additional level of legal compliance regarding cyber security. Their compliance to NIS regulations must be routinely audited by a defined competent authority.

13. For NHS boards in Scotland, this function is being fulfilled by the SG through the Scottish Health Competent Authority (the Health CA). The Drinking Water Quality Regulator for Scotland fulfils this function for Scottish Water. The results of these reviews are reported annually to Scottish Ministers.

14. A significant revision to the EU NIS Regulations (NIS2) is expected to come into force during the latter half of 2024. In addition to expanding the range of public sector bodies that are considered to be OES, an increased range of controls will be introduced.

Future Networks for Government (FN4G)

15. The Public Services Network (PSN) is a legacy network used extensively by local government. To maintain their connection to PSN organisations were required to have annual independent assessment of their operation and cyber security arrangements. The PSN has become dated and progressively more difficult to secure consequently it will be replaced by Future Networks for Government (FN4G) in due course.

16. As part of FN4G the UK Cabinet Office is encouraging organisations to migrate to modern network solutions, which offer improved security, greater flexibility and scalability.

Evidence and reporting

Audit evidence

17. Under each of the frameworks, bodies should have some form of independent accreditation on part of their arrangements. For example:

- Under the PSCRF, central government bodies should have some independent accreditation, e.g. cyber essentials plus.
- NHS bodies will have been subject to an audit by the Scottish Health Competent Authority (outsourced to a contractor).
- Local government bodies should have an annual independent assessment as part of PSN accreditation.

18. The above is audit evidence that auditors may wish to request.

19. Progression in compliance against the framework (e.g. cyber security maturity) can be measured over a number of years. Auditors should be able to see evidence of action plans to address risks and gaps identified.

Reporting

20. Where auditors identify cyber risks, any discussions at Board/Audit Committee meetings should make reference to the appropriate frameworks.

21. Due to the comprehensive and sensitive nature of the evidence and reporting, auditors may wish to consider the level of detail included in their Annual Audit Report. It is suggested that assessment and comment should focus on local governance arrangements and how public bodies are addressing the identified risks.

22. Specific detail of identified risks should be avoided (unless the risk is considered pertinent to an audit opinion).

Appendix 1: Resources

The following list provides some additional background references:

- Cyber-Assessment-Framework-v3-1.pdf – from www.ncsc.gov.uk – "*provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.*"

- https://www.cyberscotland.com/ - branded as "*The best place to find up to the minute cyber services information across Scotland*"

- Future Networks for Government (FN4G) – from www.gov.uk – details of "*the Cabinet Office programme set up to help organisations move away from PSN*".

Appendix 2: PSCRF standards

The PSCRF was designed to aggregate the controls of a variety of cyber security standards into a single framework. Version 2 of the PSCRF is currently being developed to aggregate the controls in the following standards:

- Cyber Essentials: 2022 (revised)
- Public Sector Action Plan
- Digital First
- 10 Steps (revised)
- UK GDPR Security Outcomes
- NIS-CAF 3.1 (revised)
- ISO 27002:2022 (revised)
- BS 3111:2018 (new)
- CSA STAR / Cloud Control Matrix (CCM) (new)
- ETSI EN 303 645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements (new)

NOTE: As the PSCRF is being refined at the date of preparing this guidance, additional standards may be included in the final publication.

Guidance on Cyber Security Arrangements

for 2022/23 Annual Audits

Audit Scotland's published material is available for download on the website in a number of formats. For information on our accessibility principles, please visit:
www.audit-scotland.gov.uk/accessibility

For the latest news follow us on social media or
subscribe to our email alerts.

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500 Email: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

AS.4.0